NAME

ffproxy — filtering HTTP/HTTPS proxy server

SYNOPSIS

ffproxy [**-p** *port*] [**-c** *ip|hostname*] [**-C** *ip|hostname*] [**-l** *childs*]
[**-u** *uid|user* **-g** *gid|group*] [**-r** *dir*] [**-D** *datadir*]
[**-x** *proxyip|proxyhost* **-X** *proxyport*] [**-a** *ip|hostname*] [**-A** *port*]
[**-f** *configfile*] [**-ds4bBhv**]

DESCRIPTION

ffproxy is a filtering HTTP/HTTPS proxy server. It is able to filter by host, URL, and header. Custom header entries can be filtered and added. It can even drop its privileges and optionally `chroot`(2) to some directory. Logging to `syslog`(3) is supported, as is using another auxiliary proxy server. An HTTP accelerator feature (acting as a front-end to an HTTP server) is included. Contacting IPv6 servers as well as binding to IPv6 is supported and allows transparent IPv6 over IPv4 browsing (and vice versa).

Remind that there is an alternative to command line options by using configuration files. See `ffproxy.conf`(5) and `sample.config` for details. It allows options that are not available on command line.

The following command line options are recognized. They specify general settings like IP to bind to or place of the db/ and html/ directories. Note that arguments to options must be seperated from the option by spaces, as are such options from each other.

-p *port*
Bind to port. Default is 8080.

-c *ip|hostname*
Bind to IPv4. Default is any IPv4.

-C *ip|hostname*
Bind to IPv6. Default is any IPv6.

-l *childs*
Maximum number of child processes to be forked. That is, the maximum number of concurrent requests allowed. Default is 10.

-u *uid|user* **-g** *gid|group*
Change UID and GID. Both options must be used. Default is not changing UID and GID.

-r *dir* Change root `chroot`(7) to dir. Used in conjunction with -u and -g. Because ffproxy drops its privileges and chroots after reading the configuration files, -D should be set to . (the current dir). It might need `/etc/resolv.conf` copied as etc/resolv.conf in its working directory. Example: “# cd /var/ffproxy ; /usr/local/bin/ffproxy -r /var/ffproxy -D . -d -u proxy -g proxy -f ""”

-x *ip|hostname*
Specify IP (or hostname) of an auxiliary proxy server that the program will forward requests to. Used together with -X.

-X *port*
Port number of auxiliary proxy.

-D *dir* Location of the db/ and html/ directories. For example, specifying -D /var/ffproxy tells the proxy to search for db/ files in `/var/ffproxy/db/` and html/ files in `/var/ffproxy/html/`.

-a *ip|hostname*
Auxiliary forward HTTP server to use (see section HTTP ACCELERATOR).

−A *port*
Port to use for above. Defaults to 80.

−f *configfile*
User configuration file to load. Please note that command line options get overwritten by set configuration file options. Default location is `/usr/local/etc/ffproxy.conf`. Read `ffproxy.conf`(5) for details. Use -f "" to disable configuration files.

−d Run as daemon.

−s Be silent. Don't log to syslog.

−4 Use IPv4 only. Do not try contacting servers via IPv6.

−b Don't bind to IPv4. Might be needed under Linux 2.4, due to a ''Feature'' IPv6 binds to IPv4, too. Try using this option or bind to specific IPv6 address via -C.

−B Don't bind to IPv6.

−h Show usage information.

−v Display version number.

THE DB/ DIRECTORY

The db/ directory contains files that control the behaviour of ffproxy. The files for filtering are prefixed by 'filter'. Access to the proxy server is controlled by files with prefix 'host'.

Filtering

Requests or header entries to be filtered are matched by extended regular expressions or case insensitive by strings.

ffproxy is able to filter requests by host, header, remote header, and URL. The specific files are

filter.host.match
filter.header.drop
filter.header.entry
filter.header.match
filter.rheader.drop
filter.rheader.entry
filter.rheader.match
filter.url.match

Files ending in 'drop' specify requests to be completely filtered (dropped). Files ending in 'entry' specify header entries to be removed from the header. They are matched case insensitive without extended regular expressions. Files ending in 'match' specify extended regular expressions to be matched against header entries, host, or URL.

Adding custom header entries is also supported. The entries of file `filter.header.add` will be added to every outgoing request.

Access Control

Access to the proxy is controlled through the files prefixed 'host'.

`host.dyndns` contains host names with dynamic IPv4 addresses. The host names are resolved to IPv4 addresses and compared to the client's IP. If it matches, access is granted.

`host.ip` contains static IPv4 and IPv6 address.

`host.name` contains official hostnames (reverse lookup).

Except for `host.dyndns`, the files contain extended regular expressions. If any of the entries matches, access is granted.

Layout of db/ Files

Every mentioned file above must exist, although it may be empty. Every entry is exactly one line. Empty lines are ignored, as are lines beginning with a # (comments).

The location of the db/ directory may be specified by an argument to the command line option -D. If this option and configuration file option db_files_path are not used, ffproxy will search for db/ and html/ in `/usr/local/share/ffproxy`.

ffproxy comes with sample db/ files. They also contain needed and suggested entries, as described next.

Suggested db/ file entries

The file `filter.header.entry` should contain following entries for the program's proper operation

```
Accept-Encoding:
Accept:
Connection:
Proxy-Connection:
Host:
```

First two lines are needed for browsers that send out Accept*: Headers but don't understand encoded data coming back from the proxy. Host: has to be removed, since proxies require absolute URIs (Host: is redundant).

`filter.header.add` should contain

```
Connection: close
Proxy-Connection: close
```

We removed the two entries through `filter.header.entry` and now implant our own to force disconnection after each request.

`filter.rheader.entry` should contain

```
Connection:
Proxy-Connection:
```

Whatever the server answered, we remove it.

THE HTML/ DIRECTORY

This directory contains files with HTTP header and HTML that are sent to the user's browser if either an error occured or a request was filtered. In the files, the variable *$u* will be replaced by the URL, *$h* by the host to connect to, and *$c* by the hostname of the client.

Since the files are loaded into memory for faster execution, the size of each file is limited to about 8 kB (what is more than enough, the default files are under 1 kB).

The specific files are (every file must exist)

connect	Connection failed (503)
filtered	Request filtered (200)
invalid	Invalid request (400)

post	Unable to post data (400)
resolve	Resolve error (503)

HTTP ACCELERATOR

ffproxy may also be used as a HTTP accelerator, that is, connecting to just one HTTP server and beeing a front-end to that. Use accel_host and accel_port in configuration file or command line options -a and -A to use this feature.

Default behaviour is *not* sending Host: header to allow insertion of a custom one via `filter.header.add` (see section THE DB/ DIRECTORY) or keeping the original one used by connecting client (‘Host:’ hast to be removed from default `filter.header.entry`, of course). To change this, use ‘accel_user_host no’ in the configuration file. “Host: accel_host:accel_port” will be used then.

TRANSPARENT OPERATION

It is possible to redirect all HTTP traffic, that is, traffic to port 80, to the proxy’s listening port. It will then transparently act as a HTTP proxy, the client not even knowing it is connecting to a proxy.

On OpenBSD one could enable this by adding a line like

```
rdr on rl0 proto tcp from any to any port 80 -> 127.0.0.1 port 8080
```

to `/etc/pf.conf`. In this example, rl0 is the local interface. All traffic coming from rl0 directed to port 80 (HTTP standard port) is sent to 127.0.0.1:8080 where ffproxy is supposed to be listening.

KEEP ALIVE

The program supports keep alive on client to proxy connections. This is used automatically by default and may be disabled by setting ‘use_keep_alive no’ in the configuration file.

HTTPS OPERATION

The proxy allows HTTPS proxying via implementation of the CONNECT request method. By default, only port 443 is allowed for CONNECT. This may be changed by using ‘unrestricted_connect yes’ in the configuration file. Timeout may also be tuned by ‘timeout_connect seconds’.

RELOADING CONFIGURATION

Send a SIGHUP to the pid of the ffproxy master process to let it reload db/ files, html/ files, *and* configuration file. If no configuration file was specified, `/usr/local/etc/ffproxy.conf` is tried. Of course, only some changes to the program can be done at runtime. See `ffproxy.conf`(5) for details on options that may be changed at runtime.

If daemonized, the master process writes the pid file `ffproxy.pid` to the working directory, that is, the directory specified by db_files_path or the command line parameter -D. It defaults to `/usr/local/share/ffproxy`. The program will terminate if writing fails.

LOGGING

By default, the proxy logs incorrect and filtered requests. To log all requests, use the configuration file keyword ‘log_all_requests yes’. Please make sure that you seperate the programs log output from that of other programs by modifying `syslog.conf`(5), since the output is very noisy.

FILES

Behaviour of ffproxy is determined by

- startup options given either on the command line or read from configuration files -- `/usr/local/etc/ffproxy.conf` is loaded by default.

- the files in db/ which specify filtering options and who is allowed to connect and use ffproxy

If daemonized, ffproxy writes the pid of its master process to the file named `ffproxy.pid` in its working directory -- `/usr/local/share/ffproxy` by default.

SEE ALSO

`sample.config` for a sample configuration file

`/usr/local/etc/ffproxy.conf` for default configuration file

`ffproxy.conf`(5) for details on config file

`ffproxy.quick`(7) for a short description of how to set up the proxy

`http://faith.eu.org/programs.html` for latest version and patches

`regex`(7), `re_format`(7), `syslogd`(8), `chroot`(2), `kill`(1)

CONTRIBUTORS

Dobrica Pavlinusic <dpavlin@rot13.org> provided patches for http accelerator feature

VERSION

This manual documents ffproxy 1.6 (2005-01-05).

Send bug reports, comments, suggestions to <niklas@noxa.de>

AUTHOR

Niklas Olmes <niklas@noxa.de>